UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/782,593	02/12/2001	Marc VanHeyningen	PA4404US	9483

22830 7590 09/18/2007

CARR & FERRELL LLP
2200 GENG ROAD
PALO ALTO, CA 94303

EXAMINER	
SHAW, YIN CHEN	
ART UNIT	**PAPER NUMBER**
2135	
MAIL DATE	**DELIVERY MODE**
09/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/782,593	VANHEYNINGEN, MARC	
	Examiner	Art Unit	
	Yin-Chen Shaw	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 June 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5,7-9,16-21,23-26,28-33 and 35-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *7-9,16-21,23-26,28,29 and 35-37* is/are allowed.

6)☒ Claim(s) *1-3, 5, and 30-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This written action is responding to the Request for Continued Examination (RCE) dated on 06/27/2007.
2. Claims 1, 3, 7, 16, 23, 30, 32, and 35 have been amended. Claims 4, 6, 10-15, 22, 27, 34, and 38-67 have been canceled.
3. Claims 1-3, 5, 7-9, 16-21, 23-26, 28-33, and 35-37 have been submitted for examination.
4. The Office would like to notify the Applicant that there has been a change in the Examiner to conduct the future examination and prosecution process of the currently pending application.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 5, 30, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Binding et al. (U.S. Patent 6,775,772) and further in view of Djakovic (U.S. Patent 6,351,539).

   a. *Referring to Claim 1:*

      As per Claim 1, Binding et al. disclose a method of transmitting data securely over a computer network, comprising the steps of:

(1) establishing a communication path between a first computer and a second computer **[(Fig. 3)]**;

(2) encrypting and transmitting data records between the first computer and the second computer using an unreliable communication protocol **[(lines 22-25, Col. 14 and lines 45-48, Col. 14 and Fig. 3)]**, wherein each data record incorporates a nonce and encrypted text that has been encrypted using the nonce and a shared encryption key and without reference to a previously transmitted data record **[(lines 33-41, Col. 14)]**; and

(3) in the second computer, receiving and decrypting the data records transmitted in step (2) by, for each of the received data records, decrypting the incorporated encrypted text using the incorporated nonce in combination with the shared encryption key and without reference to a previously received data record **[(lines 42-48, Col. 14)]**.

Binding et al. do not expressly disclose the remaining limitation of the claim. However, Djakovic et al. disclose the step of, in the second computer, verifying for each received data record that the incorporated nonce has not previously been received in a previously transmitted data record **[(lines 35-44, Col. 5); *where random number generator is a true random sequence generators which have the property that the random sequences cannot be reproduced*]**.

Binding et al. and Djakovic et al. are from similar technology relating to security for the digital content and data. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Binding et al. and Djakovic et al. since one would be motivated to increase the security provided by any single block cipher by providing encryption of an input stream by at least two different block ciphers (lines 12-14, Col. 2 from Djakovic). Therefore, it would have been obvious to combine Binding et al. with Djakovic et al. to obtain the invention as specified in claim 1.

b. *Referring to Claim 5:*

As per Claim 5, Binding et al. with Djakovic et al. disclose the method of claim 1, wherein the nonce comprises a random number **[(14, Fig. 1 and lines 35-44, Col. 5)]**.

c. *Referring to Claim 30:*

As per Claim 30, Binding et al. disclose a method of transmitting data securely over a computer network, comprising:

establishing a communication path with a remote computer **[(Fig. 3)]**;

receiving data records transmitted from the remote computer using an unreliable communication protocol **[(lines 22-25, Col. 14 and lines 45-48, Col. 14 and Fig. 3)]**, and

encrypted using a nonce and a shared encryption key such that each data record incorporates a nonce and text that is encrypted without

reference to a previously encrypted data record **[(lines 33-41, Col. 14)]**; and

decrypting the received data records by using the nonce in combination with a previously shared encryption key to decrypt each received data record without reference to a previously received data record **[(lines 42-48, Col. 14)]**.

Binding et al. do not expressly disclose the remaining limitation of the claim. However, Djakovic et al. disclose verifying that the nonce has not previously been received in a previously received data record **[(lines 35-44, Col. 5); *where random number generator is a true random sequence generators which have the property that the random sequences cannot be reproduced*]**. Binding et al. and Djakovic et al. are from similar technology relating to security for the digital content and data. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Binding et al. and Djakovic et al. since one would be motivated to increase the security provided by any single block cipher by providing encryption of an input stream by at least two different block ciphers (lines 12-14, Col. 2 from Djakovic). Therefore, it would have been obvious to combine Binding et al. with Djakovic et al. to obtain the invention as specified in claim 30.

d. *Referring to Claim 33:*

As per Claim 33, the rejection of Claim 30 is incorporated. In addition, Claim 33 encompasses limitations that are similar to those of Claim 5. Therefore, it is rejected with the same rationale applied against Claim 5 above.

6. Claims 2-3 and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Binding et al. (U.S. Patent 6,775,772) and Djakovic (U.S. Patent 6,351,539), and further in view of King (U.S. Patent 6,317,381).

a. *Referring to Claim 2:*

As per Claim 2, Binding et al. with Djakovic et al. disclose the method of claim 1. Binding et al. with Djakovic et al. do not expressly disclose the remaining limitations of the claim. However, King et al. further comprising the step of, prior to step (1) establishing a reliable communication path between the first computer and the second computer and exchanging security credentials over the reliable communication path **[(lines 39-41, Col. 4 and lines 4-20, Col. 7 from King)]**. The

Binding et al., Djakovic et al., and King are from similar technology relating to security for the digital content and data. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Binding et al. and Djakovic et al. with King since one

would be motivated to provide improved approaches to to provide secure data transmissions over one-way channels (lines 21-22, Col. 3 from King). Therefore, it would have been obvious to combine Binding et al. and Djakovic et al. with King to obtain the invention as specified in claim 2.

b. *Referring to Claim 3:*

As per Claim 3, Binding et al., Djakovic et al., and King disclose the method of claim 2, wherein the step of exchanging security credentials comprises the step of exchanging the shared an encryption key that is used to encrypt the data records in step (2) **[(lines 22-25, Col. 14 from Binding et al.) and (lines 39-41, Col. 4 and lines 4-20, Col. 7 from King)]**.

c. *Referring to Claim 31:*

As per Claim 31, the rejection of Claim 30 is incorporated. In addition, Claim 31 encompasses limitations that are similar to those of Claim 2. Therefore, it is rejected with the same rationale applied against Claim 2 above.

d. *Referring to Claim 32:*

As per Claim 32, the rejection of Claim 31 is incorporated. In addition, Claim 32 encompasses limitations that are similar to those of Claim 3. Therefore, it is rejected with the same rationale applied against Claim 3 above.

Allowable Subject Matter

7. Claims 7-9, 16-21, 23-26, 28-33, and 35-37 are allowable subject matter.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

    a. Howard et al. (U.S. Pub. 20020118836) disclose first and second computing devices are selectively operatively coupled together. The first device provides data to the second device. The second device can be a portable computing device. The second device is configured to encrypt/decrypt the data, as needed by the first device. The second device maintains the cryptographic key data internally. As such, the first device, which, for example, may be a personal computer will only maintain the returned encrypted data following encryption and only temporarily use any returned decrypted data. Thus, by physically and operatively distributing the cryptographic processing/maintenance between the two devices, additional security is provided for protecting private data.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yin-Chen Shaw whose telephone number is 571-272-8593. The examiner can normally be reached on 8:30 to 4:30 M-F. If

attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Yen Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

YCS

Sep. 17, 2007

KIM VU
SUPERVISORY PATENT EXAMINE
TECHNOLOGY CENTER 2100